Report for: jefferymcbride87@gmail.com

As of 2024-08-10T16:15:39.885Z

Minified and concise search report.

Module Responses:

TWITTER

Registered: true

XVIDEOS

Registered: true

PINTEREST

Registered: true

ESPN

Registered: true

HIBP

Picture Url

Registered: true
Breach: true
Name: ApexSMS
Bio: In May 2019, news broke of a massive SMS spam operation

known as "ApexSMS" which was discovered after a MongoDB instance of the same name was found exposed without a password. The incident leaked over 80M records with 23M unique email addresses alongside names, phone numbers and carriers, geographic locations (state and country), genders and IP addresses.

Creation Date: 2019-04-15T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png

Description: In May 2019, news broke of a massive SMS spam operation known as "ApexSMS" which was discovered after a MongoDB instance of the same name was found exposed without a password. The incident leaked over 80M records with 23M unique email addresses alongside names, phone numbers and carriers, geographic locations (state and country), genders and IP addresses.

Title: ApexSMS

Breach Count: 23246481

HIBP

Picture Url

Registered: true

Breach: true

Name: AT&T

Bio: In March 2024, tens of millions of records allegedly breached from AT&T were posted to a popular hacking forum. Dating back to August 2021, the data was originally posted for sale before later being freely released. At the time, AT&T maintained that there had not been a breach of their systems and that the data originated from elsewhere. 12 days later, AT&T acknowledged that data fields specific to them were in the breach and that it was not yet known whether the breach occurred at their end or that of a vendor. AT&T also proceeded to reset customer account passcodes, an indicator that there was sufficient belief passcodes had been compromised. The incident exposed names, email and physical addresses, dates of birth, phone numbers and US social security numbers.

Creation Date: 2021-08-20T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ATT.png

Description: In March 2024, tens of millions of records allegedly breached from AT&T were posted to a popular hacking forum. Dating back to August 2021, the data was originally posted for sale before later being freely released. At the time, AT&T maintained that there had not been a breach of their systems and that the data originated from elsewhere. 12 days later, AT&T acknowledged that data fields specific to them were in the breach and that it was not yet known whether the breach occurred at their end or that of a vendor. AT&T also proceeded to reset customer account passcodes, an indicator that there was sufficient belief passcodes had been compromised. The incident exposed names, email and physical addresses, dates of birth, phone numbers and

US social security numbers.
Title: AT&T
Breach Count: 49102176

HIBP

Picture Url

Registered: true
Breach: true
Name: Combolists Posted to Telegram
Bio: In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.
Creation Date: 2024-05-28T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.
Title: Combolists Posted to Telegram
Breach Count: 361468099

HIBP

Picture Url

Registered: true
Breach: true
Name: Data Enrichment Exposure From PDL Customer
Bio: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Creation Date: 2019-10-16T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In October 2019, <a href="https://www.troyhunt.com/data-enrichment-people-data-

labs-and-another-622m-email-addresses" target="_blank" rel="noopener">security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Title: Data Enrichment Exposure From PDL Customer
Breach Count: 622161052

HIBP

Picture Url

Registered: true
Breach: true
Name: Dubsmash
Website: dubsmash.com
Bio: In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Creation Date: 2018-12-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Dubsmash.png
Website: dubsmash.com
Description: In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Title: Dubsmash
Breach Count: 161749950

HIBP

Picture Url

Registered: true
Breach: true
Name: Instant Checkmate
Website: instantcheckmate.com

Bio: In 2019, the public records search service Instant Checkmate suffered a data breach that later came to light in early 2023. The data included almost 12M unique customer email addresses, names, phone numbers and passwords stored as scrypt hashes.
Creation Date: 2019-04-12T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/InstantCheckmate.png
Website: instantcheckmate.com
Description: In 2019, the public records search service Instant Checkmate suffered a data breach that later came to light in early 2023. The data included almost 12M unique customer email addresses, names, phone numbers and passwords stored as scrypt hashes.
Title: Instant Checkmate
Breach Count: 11943887

HIBP

Picture Url

Registered: true
Breach: true
Name: Lumin PDF
Website: luminpdf.com
Bio: In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2019-04-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/LuminPDF.png
Website: luminpdf.com
Description: In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Title: Lumin PDF
Breach Count: 15453048

HIBP

Picture Url

Registered: true
Breach: true
Name: Modern Business Solutions
Website: modbsolutions.com
Bio: In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.
Creation Date: 2016-10-08T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ModernBusinessSolutions.png
Website: modbsolutions.com
Description: In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.
Title: Modern Business Solutions
Breach Count: 58843488

HIBP

Picture Url

Registered: true
Breach: true
Name: Nitro
Website: gonitro.com
Bio: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of

converted documents. The data was provided to HIBP by dehashed.com.
Creation Date: 2020-09-28T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Nitro.png
Website: gonitro.com
Description: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Title: Nitro
Breach Count: 77159696

HIBP

Picture Url

Registered: true
Breach: true
Name: ParkMobile
Website: parkmobile.io
Bio: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.
Creation Date: 2021-03-21T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ParkMobile.png
Website: parkmobile.io
Description: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.
Title: ParkMobile
Breach Count: 20949825

HIBP

Picture Url

Registered: true
Breach: true
Name: River City Media Spam List
Website: rivercitymediaonline.com
Bio: In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.
Creation Date: 2017-01-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png
Website: rivercitymediaonline.com
Description: In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.
Title: River City Media Spam List
Breach Count: 393430309

HIBP

Picture Url

Registered: true
Breach: true
Name: Straffic
Website: straffic.io
Bio: In February 2020, Israeli marketing company Straffic exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders. In their breach disclosure message, Straffic stated that "it is impossible to create a totally immune system, and these things can occur".
Creation Date: 2020-02-14T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Straffic.png
Website: straffic.io
Description: In February 2020, Israeli marketing company Straffic exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders. In their breach disclosure message, Straffic stated that "it is impossible to create a totally immune

system, and these things can occur".
Title: Straffic
Breach Count: 48580249

HIBP

Picture Url

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Creation Date: 2021-01-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Twitter.png
Website: twitter.com
Description: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Title: Twitter (200M)
Breach Count: 211524284

HIBP

Picture Url

Registered: true
Breach: true
Name: Verifications.io
Website: verifications.io
Bio: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a

password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Creation Date: 2019-02-25T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/VerificationsIO.png

Website: verifications.io

Description: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Title: Verifications.io

Breach Count: 763117241

HIBP

Picture Url

Registered: true

Breach: true

Name: Zynga

Website: zynga.com

Bio: In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Creation Date: 2019-09-01T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Zynga.png

Website: zynga.com

Description: In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Title: Zynga

Breach Count: 172869660

CYBERBACKGROUNDCHECKS

Registered: true
Name: Jeffery Wayne Mcbride JR
Age: 37
Location: 100 Anabel Ave, Saint Louis, MO, 63135, US
Email: nmcbride@aol.com, mahanbrooke@yahoo.com, jefferymcbride87@gmail.com, jfizzleproductions@netzero.net, mcbridejeffery@gmail.com, lsmithnsg@msn.com, lauracarlson@live.com, jfizzleproductions@yahoo.com, tru_2_da_game87@yahoo.com, anthony77525@yahoo.com, ghetto_mix_boy@yahoo.com, ghettomixboy@yahoo.com, plumer_99@yahoo.com, ajfizzleproductionsz34@yahoo.com, lmcmaster406@comcast.net, mc406@wmconnect.com, j_fizzle_4shizzle@earthlink.net, jream@bellatlantic.net, nmcbride68@aol.com, jeffery.mcbride@iwon.com, anita.mcbride@bellsouth.net
Phone: (573) 221-2678, (573) 221-1688, (573) 406-1573, (415) 846-8800, (440) 570-8284, (573) 719-3335, (314) 521-2225, (573) 221-5781, (573) 822-3096, (816) 853-5496, (573) 221-7000, (573) 221-8929, (573) 795-4249
Other Names: Jeffery W Mcbride JR, Jeffery Wayne Mcbride, Jeffery W Mcbride, Jeffery Mcbride, Jeffery M Mcbride, Jeffery Mcbride JR, Jefferyw Mcbride JR, Jeffery Mcbrde, Jeffrey W Mcbride, Jeffrey Mcbride, Jeff W Mcbride, Jaffery Mcbride, Jefferyw Mcbride, Jeffery Wayne, Jeffrey Mcbride JR, Jeff Mcbride, Jefferey Mcbride, Jeffery Undefined Mcbride JR, Jeffery Mcbrode, Jeffrey Mc Bride, Jeff Mc Bride, Jeff Mc
Results Page: https://www.cyberbackgroundchecks.com/detail/jeffery-wayne-mcbride/pidnazpgallmzqapgagxypm

---

DISNEYSTORE

Registered: true

PANDORA

Picture Url
Profile Url

Registered: true
Username: jefferymcbride87
Followers: 0
Following: 0
Likes: 1
Stations: 1

APPLE

Registered: true

MICROSOFT

Registered: true
Id: A729BCC0E9E8EB21
Name: jefferymcbride87@gmail.com
Last Seen: 2019-10-08T00:09:14.657000+00:00
Creation Date: 2016-04-29T17:21:29.297000+00:00

DROPBOX

Registered: true

YOUTUBE

Picture Url
Profile Url

Registered: true
Id: UClmC3mrd1uZbR7RukSvCg6w
Name: Jeffery Mcbride
Subscriber Count: 6
Joined Date Indication: 10 years ago

LINKEDIN

Registered: true

MAPS

Profile Url

Registered: true
Private: false

GOOGLE

Picture Url

Registered: true
Id: 104100190879599228130
Name: Jeffery Mcbride
Last Seen: 2023-10-27T04:20:25
